CENTRUM USŁUG INFORMATYCZNYCH
WE WROCŁAWIU

Centrum Usług Informatycznych we Wrocławiu
ul. Namysłowska 8, 50-304 Wrocław

Wrocław, 09.10.2024

Dotyczy: postępowania prowadzonego w trybie podstawowym bez negocjacji, pn.: **„Zakup Systemu Kadrowo-Płacowego i finansowo - księgowy dla ZZM i ZZK”**, znak postępowaniaCUI-ZZ.3200.29.2024

Zamawiający informuje, że do przedmiotowego postępowania wpłynęły wnioski o treści jak poniżej. Zamawiający, na podstawie art. 284 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.) – dalej ustawa Pzp, przekazuje odpowiednio: odpowiedzi na wnioski o wyjaśnienie treści SWZ i/lub zmienia treść SWZ:

Pytanie nr 1:
„W „Załącznik nr 1 do projektu umowy – Opis Przedmiotu Zamówienia” w rozdziale 1 „Cel i ogólny opis projektu” Zamawiający opisuje zasady zrzutu danych z wdrożonego sytemu wymieniając akceptowalne formaty: np. CSV, JSON, XML oraz wymagając kompletności eksportowanych danych. Mając na uwagę duży zakres informacji przechowywanych w systemie proponujemy, aby Zamawiający dopuścił zrzut danych w postaci bazy danych typu SQL, pod warunkiem że Wykonawca zapewni, że przekaże opis struktury bazy SQL oraz zapewni wraz ze zrzutem licencję na bazę danych wraz z opisem jej instalacji bazy lub dostarczy zrzut na maszynie wirtualnej z zainstalowanym oprogramowaniem bazy danych, z wymaganymi licencjami i odtworzoną bazą. W naszej ocenie takie równoważne rozwiązanie zapewni Zamawiającemu kompletność zrzutu danych i pozwoli uniknąć ewentualnych błędów związanych z konwersją danych do formatów CSV, JSON,XML"

Odpowiedź:
Zamawiający dopuści zrzut danych opisany jak powyżej jeżeli Wykonawca zapewni, że w bazę danych będzie wbudowana funkcjonalność pozwalająca na eksport danych do wcześniej wskazanych formatów.

Zamawiający, na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych, zmienia treść SWZ, w ten sposób, że: w Załączniku nr 1 do Umowy – OPZ, w rozdziale 1 „Cel i ogólny opis projektu” zmienia zapis dotyczący **pkt. 2 „Metoda zrzutu danych”** z:

„- Dane ze zrzutu muszą być zapisane w standardowych, powszechnie akceptowanych formatach (np. CSV, JSON, XML)” na:

Nowe brzmienie zapisu:

„- Dane ze zrzutu powinny być zapisane w standardowych, powszechnie akceptowanych formatach (np. CSV, JSON, XML), możliwy jest również zrzut bazy danych bez konwersji do tych formatów jeżeli Wykonawca zapewni dokładny opis struktur bazy danych w dokumentacji oraz wbudowaną w bazę funkcjonalność, która umożliwi Zamawiającemu eksport do wyżej wymienionych formatów lub innego wskazanego w Rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773)”

Pytanie nr 2:
„ad WTA.10:
System musi umożliwiać zmianę hasła użytkownika przez administratora aplikacji poprzez wprowadzenie nowego hasła dla użytkownika. W takim przypadku użytkownik, któremu zmieniono hasło przy pierwszym logowaniu do Systemu musi zostać zmuszony przez System do zmiany hasła (na tylko sobie znane). Rozwiązanie może zostać zastąpione równoważnym po zatwierdzeniu innego rozwiązania przez Zamawiającego. Użytkownik może sam zresetować hasło, np. poprzez „Funkcję przywracania hasła”.
Prosimy o potwierdzenie, ze użytkownik może samodzielnie resetować hasło np. poprzez „Funkcję przywracania hasła” należy czytać łącznie ze zdaniem „Rozwiązanie może zostać zastąpione równoważnym po zatwierdzeniu innego rozwiązania przez Zamawiającego.” lub potwierdzenie, że funkcja samodzielnej zmiany hasła może dotyczyć tylko Użytkowników portalu pracownika."

Odpowiedź:
Zamawiający dopuszcza podaną równoważność dla użytkowników obsługujących system polegającą na samodzielnym zresetowaniu hasła, np. poprzez „Funkcję przywracania hasła” pod warunkiem dostępu do funkcji po autoryzacji lub innego mechanizmu zabezpieczającego uzgodnionego w analizie systemowe.
Zamawiający informuje, że funkcje samodzielnej zmiany hasła i przywrócenia hasła są rozdzielne i bezwzględnie wymagane dla Użytkowników portalu pracownika.

Pytanie nr 3:
„ad WTA.22:
„Wszystkie zgłoszenia dotyczące obsługi Systemu oraz Awarii będą ewidencjonowane i rozwiązywane przy pomocy narzędzia serwisowego Zamawiającego – HelpDesk. (Jeżeli Wykonawca posiada swój własny system

serwisowy, istnieje możliwość integracji w celu wymiany danych z serwisem Zamawiającego.)”
Prosimy o dopuszczenie aby zgłoszenia mogły być rejestrowane w narzędziu własnym Wykonawcy, zintegrowanym z jego Systemem, które pozwoli na rejestrację zgłoszeń bezpośrednio z użytkowanego systemu (bez konieczności dodatkowego logowania do systemu zgłoszeniowej Wykonawcy) oraz umożliwi zdefiniowanym Użytkownikom Zamawiającego przeglądanie z poziomu przeglądarki internetowej i kontrolowanie zarejestrowanych zgłoszeń w podziale na poszczególnych Użytkowników."

Odpowiedź:
Zamawiający nie wyraża zgody na zmianę narzędzia serwisowego HelpDesk. Treść wymagania pozostaje bez zmian.

Pytanie nr 4:
„ad WTA.26
System musi umożliwiać nadawanie uprawnień tylko do poszczególnych funkcjonalności, modułów, raportów, pól.
Ponieważ nadawanie uprawnień do poszczególnych pól może być różnie rozumiane i może powodować ewentualne komplikacje na etapie realizacji Zamówienia, prosimy aby Zamawiający usunął wymaganie dot. nadawania uprawnień do pól lub zezwolił aby lista pól została do których będą nadawane uprawnienia zostały określone na etapie analizy."

Odpowiedź:

Zamawiający, na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych, zmienia treść SWZ, w ten sposób, że: w Załączniku nr 1 do Umowy – OPZ, w tabeli **Wymagania techniczne i administracyjne – zadanie nr 1 i 2**, w wierszu **WTA.26** w kolumnie „Opis wymagania” wykreśla treść:

„System musi umożliwiać nadawanie uprawnień tylko do poszczególnych funkcjonalności, modułów, raportów, pól.”

Nowe brzmienie wiersza **WTA.26** „Opis wymagania”:

„System musi umożliwiać nadawanie uprawnień tylko do poszczególnych funkcjonalności, modułów, raportów.”

Pytanie nr 5:
„ad WTA.28:
Wskazane, aby System zapewniał administratorowi Systemu nadawanie użytkownikowi różnych ról dla różnych jednostek organizacyjnych obsługiwanych przez System.
Prosimy o potwierdzenie, że Zamawiający jako jednostki organizacyjnej rozumie dwie jednostki wymienione w przedmiocie zamówienia – tj. ZZK i ZKM lub doprecyzowanie co Zamawiający rozumie poprzez jednostkę organizacyjną."

Odpowiedź:
Zamawiający potwierdza, że jako dwie odrębne jednostki rozumie się ZZK i ZZM.

Pytanie nr 6:
„ad WTA.32:
System musi posiadać możliwość generacji „Raportu uprawnień użytkownika" w Systemie z podziałem na role. Jeśli System wymusza dodatkowo przydzielenie do danego działu (np. Działu Księgowości) lub danej jednostki to raport powinien również zawierać listę użytkowników w tym dziale, w tej jednostce. W raporcie muszą być podane co najmniej następujące informacje: login, imię i nazwisko, do jakiej jednostki użytkownik ma dostęp, jakiego rodzaju ma dostęp i do jakich danych (w tym odczyt, modyfikacja z usunięciem, wprowadzenie), do jakich funkcji w Systemie, do jakich formularzy interfejsu użytkownika.
Prosimy o potwierdzenie, że Zamawiający jako jednostki organizacyjnej rozumie dwie jednostki wymienione w przedmiocie zamówienia – tj. ZZK i ZKM lub doprecyzowanie co Zamawiający rozumie poprzez jednostkę organizacyjną.
Ponadto prosimy o potwierdzenie, że Zamawiający dopuszcza aby dane jednostek były przechowywane w niezależnych bazach, co implikowałoby że przedmiotowe raporty byłyby generowane niezależnie dla każdej z jednostek. Odwzorowanie danych poszczególnych jednostek w niezależnych bazach niesienie za sobą również wiele korzyści dot. niezależnej konserwacji, zrzutu danych, aktualizacji, które nie muszą być uzgadnianie między jednostkami."

Odpowiedź:
Zamawiający potwierdza, że jako dwie odrębne jednostki rozumie się ZZK i ZZM. Zamawiający dopuszcza rozwiązanie, gdzie będą dwie niezależne bazy dla tych jednostek i zmiany z tym związane w raportowaniu.

Pytanie nr 7:
„ad WTA.34:
Administrator aplikacji musi mieć w Systemie dostępny formularz na którym może zobaczyć jaki użytkownik jest przypisany do jakiej jednostki oraz jakie w ramach jednostki ma przypisane role lub funkcjonalność równoważna po wyrażeniu zgody przez Zamawiającego
Prosimy o potwierdzenie, że Zamawiający jako jednostki organizacyjnej rozumie dwie jednostki wymienione w przedmiocie zamówienia – tj. ZZK i ZKM lub doprecyzowanie co Zamawiający rozumie poprzez jednostkę organizacyjną.
Ponadto prosimy o potwierdzenie, że Zamawiający dopuszcza aby dane jednostek były przechowywane w niezależnych bazach, co implikowałoby że przedmiotowe raporty byłyby generowane niezależnie dla każdej z jednostek. Odwzorowanie danych poszczególnych jednostek w niezależnych bazach niesienie za sobą również wiele korzyści dot. niezależnej konserwacji, zrzutu danych, aktualizacji, które nie muszą być uzgadnianie między jednostkami."

Odpowiedź:
Zamawiający potwierdza, że jako dwie odrębne jednostki rozumie się ZZK i ZZM. Zamawiający dopuszcza rozwiązanie, gdzie będą dwie niezależne bazy dla tych jednostek i zmiany z tym związane w raportowaniu.

Pytanie nr 8:
„ad WT.1 –
System musi zostać umieszczony na zasobach dostawcy i udostępniona Zamawiającemu w modelu SaaS. Wykonawca musi zapewnić pełną dostępność oraz bezpieczeństwo działania Systemu oraz baz danych. Wykonawca powinien zapewnić separację środowisk i baz danych klientów, aby zapobiec nieuprawnionemu dostępowi i przenikaniu danych/informacji pomiędzy różnymi instancjami Systemu. Wykonawca po swojej stronie zapewni dodatkowe środki zabezpieczające System przed niepowołanym dostępem, w tym: Dla sieci publicznej/Internetu - system kontroli treści - dostęp VPN (szyfrowany dostęp zdalny) -system bezpieczeństwa usługi DNS (firewall DNS) - firewall sprzętowy, - IDS/IPS (możliwe zintegrowane w Firewall aplikacyjnym) - load balancer - dostęp do Internetu chroniony przed atakami DOS/DDOS - system kontroli dostępu do sieci wewn. (802.1x) - zabezpieczony system przydziału adresów IP system ochrony antywirusowej. Dopuszczalne jest zastosowanie innych równoważnych zabezpieczeń infrastruktury Wykonawcy po jego stronie, po wykonaniu Analizy Systemowej i akceptacji przez Zamawiającego. Wykonawca przedstawi dokumentację potwierdzającą wdrożenie i stosowanie wymienionych wyżej oraz uzgodnionych zabezpieczeń.
Ze względu na niewielkie wymagania dot. ilości Użytkowników pracujących w systemie prosimy o wykreślenie wymagania dot. load balancera, pod warunkiem zapewnienia przez Wykonawcę wydajnego rozwiązania (pozwalającego na bieżącą pracę, bez opóźnień związanych z nadmiernym obciążeniem systemu). Jednocześnie sugerujemy aby Zamawiający nie precyzował dodatkowych środków zabezpieczających System przed niepowołanym dostępem i zezwolił na ustalenie zabezpieczeń na etapie Analizy Systemowej."

Odpowiedź:

Zamawiający, na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych, zmienia treść SWZ, w ten sposób, że: w Załączniku nr 1 do Umowy – OPZ, w tabeli **Wymagania bezpieczeństwa – zadanie nr 1 i 2**, w wierszu **Wymagania Techniczne dot. Architektury Systemu i jego zasobów WT.1** w kolumnie „Opis wymagania” wykreśla treść:

„- load balancer”

Nowe brzmienie wiersza **WT.1** „Opis wymagania”:
„System musi zostać umieszczony na zasobach dostawcy i udostępniony Zamawiającemu w modelu SaaS. Wykonawca musi zapewnić pełną dostępność oraz bezpieczeństwo działania Systemu oraz baz danych. Wykonawca powinien zapewnić separację środowisk i baz danych klientów, aby zapobiec

nieuprawnionemu dostępowi i przenikaniu danych/informacji pomiędzy różnymi instancjami Systemu. Wykonawca po swojej stronie zapewni dodatkowe środki zabezpieczające System przed niepowołanym dostępem, w tym:
Dla sieci publicznej/Internetu
- system kontroli treści
- dostęp VPN (szyfrowany dostęp zdalny)
- system bezpieczeństwa usługi DNS (firewall DNS)
- firewall sprzętowy,
- IDS/IPS (możliwe zintegrowane w Firewall aplikacyjnym)
- dostęp do Internetu chroniony przed atakami DOS/DDOS
- system kontroli dostępu do sieci wewn. (802.1x)
- zabezpieczony system przydziału adresów IP system ochrony antywirusowej.
Dopuszczalne jest zastosowanie innych równoważnych zabezpieczeń infrastruktury Wykonawcy po jego stronie, po wykonaniu Analizy Systemowej i akceptacji przez Zamawiającego. Wykonawca przedstawi dokumentację potwierdzającą wdrożenie i stosowanie wymienionych wyżej oraz uzgodnionych zabezpieczeń."

Pytanie nr 9:
„ad WT.6 –
Interfejs strony internetowej (dla wszystkich modułów aplikacji) musi być obsługiwany, w najpopularniejszych przeglądarkach, np. Google Chrome, Mozilla Firefox, Microsoft Edge w wersjach wspieranych przez producenta.
Prosimy o doprecyzowanie, że Zamawiający oczekuje aby interfejs strony internetowej dot. aplikacji dostępnych z poziomu przeglądarki internetowej – tj. portalu pracownika, natomiast Zamawiający dopuszcza, aby pozostałe aplikacje były aplikacjami klienckimi uruchamianymi w środowisku Windows."

Odpowiedź:
Zamawiający potwierdza, że wymaganie dotyczy interfejsu strony internetowej. Aplikacje klienckie uruchamiane w środowisku Windows są wyłączone z tego wymagania.

Pytanie nr 10:
„ad WT.10 –
System powinien posiadać mechanizm uwierzytelniania, który pozwala użytkownikom na bezpieczne logowanie się i weryfikację tożsamości. Ponadto, system autoryzacji powinien ograniczać dostęp do funkcji i zasobów zgodnie z uprawnieniami skonfigurowanymi w Systemie. Hasła kont muszą być przechowywane tylko w postaci zahaszowanej silnym algorytmem (np. bCrypt lub równie silnym zaproponowanym przez Wykonawcę.) wraz z zastosowaniem losowo wygenerowanej soli.
Ponieważ systemy stosują różne metody przechowywania hasłem, sugerujemy aby Wykonawca zezwolił aby hasła kont mogły być przechowywane w postaci zahaszowanej silnym algorytmem z opcjonalnym zastosowaniem losowo

wygenerowanej soli. W szczególności systemy przechowywania haseł Active Directory wg naszego stanu wiedzy są zahashowane bez użycia soli. "

Odpowiedź:
Zamawiający wyraża zgodę na przechowywanie haseł w postaci zahaszowanej silnym algorytmem z opcjonalnym zastosowaniem losowo wygenerowanej soli.

Pytanie nr 11:
„ad WT.12:
System musi umożliwiać administratorowi wymuszanie zmiany hasła użytkownika poprzez generowanie jednorazowego linku do zmiany hasła, który zostanie wysłany na adres e-mail przypisany do konta użytkownika
Prosimy o dopuszczenie, że funkcja samodzielnej zmiany hasła może dotyczyć tylko Użytkowników portalu pracownika."

Odpowiedź:
Zamawiający dopuszcza realizację wymagania tylko dla Użytkowników portalu pracownika.

Pytanie nr 12:
„ad WT.13 –
Dostęp do Systemu musi być zawsze autoryzowany, co najmniej loginem i hasłem. Login (identyfikator użytkownika) musi być w Systemie unikalny i może być przydzielony tylko jednemu użytkownikowi. Po trzech nieudanych próbach logowania użytkownika w Systemie, System musi blokować konto użytkownika na okres czasu zdefiniowany przez Administratora Systemu lub ustawiony przez Wykonawcę na poziomie uzgodnionym z Zamawiającym podczas Analizy Systemowej. Konto będzie mogło zostać odblokowane przez administratora lub za pomocą rozwiązania automatycznego odblokowania po upływie czasu zdefiniowanego przez Administratora Systemu, a także za pomocą opcji „zmień hasło" generując jednorazowy link do zmiany hasła wysyłany na przypisany do użytkownika adres email
Prosimy o dopuszczenie, aby funkcja automatycznego odblokowania dostępu do konta lub samodzielnej zmiany hasła dotyczyła tylko Użytkowników portalu pracownika."

Odpowiedź:
Zamawiający dopuszcza, aby funkcja automatycznego odblokowywania dostępu do konta lub samodzielnej zmiany hasła dotyczy tylko użytkowników systemu "Portal Pracownika".

Pytanie nr 13:
„ad WT.14 –
System musi wspierać dodatkowe metody uwierzytelniania typu MFA/2FA - (np. e-mail). Włączenie mechanizmu uwierzytelniania wieloskładnikowego powinno być opcjonalnie włączane przez Administratora Systemu.

Prosimy o dopuszczenie następującego rozwiązania:

- w przypadku portalu pracownika dwuskładnikowe uwierzytelnianie definiowane będzie na poziomie użytkownika
- dla pozostałych aplikacji dwuskładnikowe uwierzytelnianie może zostać zrealizowane poprzez logowanie się poprzez dwa niezależne hasła - w pierwszej kolejności do serwera aplikacji (np. przez RDP), a następnie do właściwego Systemu"

Odpowiedź:
Dla "Portalu Pracownika" dwuskładnikowe uwierzytelnienie będzie definiowane na poziomie użytkownika. Dla pozostałych aplikacji Zamawiający wyraża zgodę na zaproponowane rozwiązanie.

Pytanie nr 14:
„ad WT.16 –
Każdy użytkownik posiadający uprawnienia logowania do Systemu musi mieć przypisane indywidualne konto w Systemie i musi zostać uwierzytelniony. W przypadku bezczynności powyżej określonej ilości minut (parametryzacja w Systemie przez administratora lub Wykonawcę na poziomie uzgodnionym z Zamawiającym w trakcie Analizy Systemowej), System musi automatycznie wylogować użytkownika.
Prosimy o dopuszczenie następującego rozwiązania:

- w przypadku portalu pracownika automatyczne wylogowanie nastąpi po określonym (zdefiniowanym przez administratora) czasie
- dla pozostałych aplikacji automatyczne wylogowanie będzie realizowane poprzez zablokowanie dostępu do pulpitu zdalnego serwera aplikacji (RDP) lub komputera"

Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane w pytaniu rozwiązanie:
- w przypadku "Portalu Pracownika" automatyczne wylogowanie nastąpi po określonym (zdefiniowanym przez administratora) czasie.
- dla pozostałych aplikacji automatyczne wylogowanie będzie realizowane poprzez zablokowanie dostępu do pulpitu zdalnego serwera aplikacji (RDP).

Pytanie nr 15:
„ad WT.18 –
Wymagany protokół HTTPS z ważnym (aktualnym) certyfikatem. Wszystkie dane przechowywane i przesyłane przez aplikację powinny być zaszyfrowane. Wymagane stosowanie silnego protokołu szyfrowania SSL (min. 2048 bit) TLS (min. 1.2), aby chronić poufne informacje przed przechwyceniem.
ad WT.26 –
System powinien szyfrować połączenia sieciowe pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
ad WT.25 –

Transmisja danych powinna podlegać ochronie kryptograficznej polegającej na szyfrowaniu. Połączenie z aplikacją i cała komunikacja pomiędzy Systemem a systemami zintegrowanymi powinna odbywać się z wykorzystaniem najnowszej wersji protokołu TLS (wersja min. 1.2) w połączeniu z Perfect Forward Secrecy umożliwiającej szyfrowanie komunikacji. Szyfrowanie zapewniać będzie, że klient może ufać certyfikatowi, który jest używany przez serwer. Klucz prywatny certyfikatu SSL będzie przechowywany na serwerze w sposób bezpieczny tzn. w konkretnym pliku zabezpieczonym odpowiednimi uprawnieniami, uniemożliwiając dostęp osobom niepowołanych (bez uprawnień).
Prosimy o dopuszczenie następującego rozwiązania:

- w przypadku portalu pracownika komunikacja będzie odbywała się zgodnie z wymaganiem Zamawiającego
- dla pozostałych aplikacji komunikacja będzie mogła odbywać się poprzez polaczenie RDP"

Odpowiedź:
Zamawiający wyraża zgodę na zaproponowane w pytaniu rozwiązanie:
- w przypadku "Portalu Pracownika" komunikacja będzie odbywała się zgodnie z wymaganiem Zamawiającego
- dla pozostałych aplikacji komunikacja będzie mogła odbywać się poprzez połączenie RDP.

Pytanie nr 16:
„ad WT.19 –
Wykonawca zastosuje wymagania prawne, organizacyjne i techniczne zapewniające bezpieczeństwo Systemu zgodnie z rekomendacjami zapisanymi w dokumencie Narodowy Standard Cyberbezpieczeństwa, w tym z integralnym Standardem Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) w aktualnej wersji, prezentowanej w bazie wiedzy serwisu www.gov.pl
Wnosimy o usunięcie tego wymagania ponieważ Zamawiający szczegółowo określił wymagania dotyczące bezpieczeństwa."

Odpowiedź:

Wymagania bezpieczeństwa zawarte w OPZ oparte są na zapisach w dokumencie "Narodowy Standard Cyberbezpieczeństwa" oraz SCCO, jednocześnie Zamawiający traktuje je jako zbiór dobrych praktyk, dlatego Zamawiający oczekuje analizy od Wykonawcy o przyjętych i odrzuconych praktykach.

Zamawiający, na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych, zmienia treść SWZ, w ten sposób, że: w Załączniku nr 1 do Umowy – OPZ, w tabeli **Wymagania bezpieczeństwa – zadanie nr 1 i 2**, w wierszu **Wymagania Techniczne dot. szyfrowania WT.19** w kolumnie „Opis wymagania” wykreśla treść:

„Wykonawca zastosuje wymagania prawne, organizacyjne i techniczne zapewniające bezpieczeństwo Systemu zgodnie z rekomendacjami zapisanymi w

dokumencie Narodowy Standard Cyberbezpieczeństwa, w tym z integralnym Standardem Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) w aktualnej wersji, prezentowanej w bazie wiedzy serwisu www.gov.pl”

Nowe brzmienie wiersza WT.19 „Opis wymagania”:
”Wykonawca przedstawi zakres stosowanych wymagań prawnych, organizacyjnych i technicznych zapewniających bezpieczeństwo Systemu na bazie rekomendacji zapisanych w dokumencie Narodowy Standard Cyberbezpieczeństwa, w tym z integralnym Standardem Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO) w aktualnej wersji, prezentowanej w bazie wiedzy serwisu www.gov.pl.”

Pytanie nr 17:
„ad WT.20a –
Dane przetwarzane w Systemie/bazie danych Systemu w spoczynku (z ang. data at rest) są szyfrowane zgodnie z aktualnymi standardami (min. Narodowy Standard Cyberbezpieczeństwa wraz z pochodnymi dokumentami w zakresie wytycznych do budowy/organizacji chmur obliczeniowych) i zgodnie z wymogami stawianymi w art. 32 ust. 1 RODO. Wykonawca jest zobowiązany do utrzymania i zarządzania aktualnymi kluczami szyfrującymi.
Długość oraz rodzaj kluczy zostanie określona podczas Analizy Systemowej. Sposób organizacji szyfrowania jest związany z wyborem technologii stosowanej przez Wykonawcę Systemu. Organizacja procesu szyfrowania danych zostanie dookreślona podczas Analizy Systemowej.

oraz ad WT.22 –
Bazy danych w zależności od wybranego modelu usługi SaaS muszą zostać skonfigurowane przez Wykonawcę tak, aby cała ich zawartość była stale zaszyfrowana (zarówno, w trakcie przechowywania w bazie danych, jak i gdy są z niej pobierane lub do niej zapisywane). Powyższy proces będzie całkowicie niewidoczny dla użytkowników, a klucze szyfrowania bezpiecznie przechowywane i zarządzane przez Musi być Wykonawcę Systemu.

oraz ad WT.23 –
Szyfrowanie danych powinno odbywać się przy użyciu klucza symetrycznego AES 256 bitów, a klucz ten powinien być zaszyfrowany parą asymetrycznych kluczy min. 2048 bitów. Zarządzanie kluczami szyfrującymi musi być dostępne zarówno dla Wykonawcy Systemu jak i zamawiającego, przy czym zamawiający obliguje Wykonawcę do pełnego zarządzania i przedłużania terminów ważności kluczy. Cały proces szyfrowania wraz z diagramem działania i wymiany kluczy szyfrowania użyty przez Wykonawcę, zostanie opisany w dokumentacji Systemu w sekcji "Informacje chronione, przeznaczone do użytku osób upoważnionych przez osobę zarządzającą po stronie Zamawiającego".

oraz WT.28 –

W ramach Analizy Systemowej określone zostaną procedury i zabezpieczenia techniczne dla bezpiecznego zarządzania kluczami obejmujące, co najmniej, następujące aspekty:

- generowanie kluczy dla różnych systemów kryptograficznych i aplikacji
- wydawanie i uzyskiwanie certyfikatów klucza publicznego
- obsługa i aktywacja kluczy dla odbiorców usług chmur obliczeniowych
- bezpieczne przechowywanie kluczy kryptograficznych
- *wymiana lub aktualizacja kluczy kryptograficznych, w tym zasad określających, w jakich warunkach i w jaki sposób wymiana i / lub aktualizacja ma być realizowana*
- wycofanie i usunięcie kluczy, na przykład w przypadku naruszenia bezpieczeństwa lub zmiany personelu
- *przechowywanie kluczy odbiorców usług chmury publicznej poza środowiskiem dostawcy usług (np. u zaufanej strony trzeciej)*

oraz ad WT.20b:
Dane przetwarzane w przesyle (z ang. data in transfer) w zakresie w jakim transfer odbywa się poza infrastrukturę informatyczną administratora – szyfrowane są zgodnie z aktualnymi standardami i zgodnie z wymogami stawianymi w art. 32 ust. 1 RODO. Wykonawca jest zobowiązany do utrzymania i zarządzania aktualnymi kluczami szyfrującymi. Długość oraz rodzaj kluczy zostanie określona podczas Analizy Systemowej. Sposób organizacji szyfrowania jest związany z wyborem technologii stosowanej przez Wykonawcę Systemu. Organizacja procesu szyfrowania da nych zostanie dookreślona podczas Analizy Systemowej.

oraz ad WT.27 –
Kryptograficzna ochrona informacji przetwarzanych powinna uwzględniać następujące zasady i instrukcje stosowania organizacyjnych i technicznych zabezpieczeń: Korzystanie z silnych algorytmów szyfrowania (np. AES), stosowanie najnowszych bezpiecznych protokołów sieciowych (np. TLS, IPsec, SSH)
Prosimy o potwierdzenie, że Zamawiający dopuszcza następujące rozwiązanie :

- dane przechowywane na serwerze bazy danych będą szyfrowane za pomocą algorytmu AES-256, a klucz zostanie zdefiniowany przez Wykonawcę na poziomie jednostki (ZZK, ZKM). Ewentualna zmiana klucza szyfrującego będzie wymagała tymczasowego deszyfrowania bazy oraz zaszyfrowania za pomocą nowego klucza.
- dla aplikacji przeglądarkowych szyfrowanie za pomocą certyfikatu TLS 1.2 lub TLS 1.3 natomiast szyfrowanie danych dla pozostałych aplikacji może odbywać się poprzez protokół RDP."

Odpowiedź:
Zamawiający informuje, że w zakresie wymienionych wymagań:
- WT.20a przedstawiona propozycja odnosi się częściowo do zakresu wymagania, zakres opisany poniżej.
- WT.22 Zamawiający informuję, że przedstawiona propozycja nie opisuje sposobu wypełnienia wymagania, a algorytm wykorzystany do szyfrowania - wymaganie WT.23.
- WT.23 Zamawiający dopuszcza zaproponowane rozwiązanie oraz dokonuje zmiany wymagania WT.23 na:

Zamawiający, na podstawie art. 286 ust. 1 ustawy Prawo zamówień publicznych, zmienia treść SWZ, w ten sposób, że: w Załączniku nr 1 do Umowy – OPZ, w tabeli **Wymagania bezpieczeństwa – zadanie nr 1 i 2**, w wierszu **Wymagania Techniczne dot. szyfrowania WT.23** w kolumnie „Opis wymagania" wykreśla treść:

„Szyfrowanie danych powinno odbywać się przy użyciu klucza symetrycznego AES 256 bitów, a klucz ten powinien być zaszyfrowany parą asymetrycznych kluczy min. 2048 bitów.Zarządzanie kluczami szyfrującymi musi być dostępne zarówno dla Wykonawcy Systemu jak i zamawiającego, przy czym zamawiający obliguje Wykonawcę do pełnego zarządzania i przedłużania terminów ważności kluczy. Cały proces szyfrowania wraz z diagramem działania i wymiany kluczy szyfrowania użyty przez Wykonawcę, zostanie opisany w dokumentacji Systemu w sekcji "Informacje chronione, przeznaczone do użytku osób upoważnionych przez osobę zarządzającą po stronie Zamawiającego"

Nowe brzmienie wiersza **WT.23** „Opis wymagania":
"Szyfrowanie danych powinno odbywać się przy użyciu algorytmu AES 256 bitów. Zamawiający obliguje Wykonawcę do pełnego zarządzania i przedłużania terminów ważności kluczy. Ewentualna zmiana klucza szyfrującego będzie możliwa za zgodą zamawiającego, co zezwoli na tymczasową deszyfrację bazy i zaszyfrowanie jej nowym kluczem (każda taka operacja powinna być raportowana Zamawiającemu). Cały proces szyfrowania wraz z diagramem działania i wymiany kluczy szyfrowania użyty przez Wykonawcę, zostanie opisany w dokumentacji Systemu w sekcji "Informacje chronione, przeznaczone do użytku osób upoważnionych przez osobę zarządzającą po stronie Zamawiającego".

Ponadto:

- WT.20b, WT.27 Zamawiający akceptuje zaproponowane rozwiązanie: dla aplikacji przeglądarkowych szyfrowanie za pomocą certyfikatu TLS 1.2 lub TLS 1.3 natomiast szyfrowanie danych dla pozostałych aplikacji może odbywać się poprzez protokół RDP.
- WT.28 - treść wymagania pozostaje bez zmian.

Działając w trybie art. 286 ust. 1 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.) Zamawiający zmienia treść SWZ, w ten sposób że:

a) zmienia termin składania i otwarcia ofert, tj. wykreśla dotychczasową treść pkt 12.1, 12.2 SWZ i nadaje im nowe brzmienie:

   „12.1. Ofertę należy składać za pośrednictwem platformy zakupowej zamieszczonej pod adresem: https://portal.smartpzp.pl/cui/public/postepowanie?postepowanie=74773623

   w terminie **do dnia 18.10.2024 r. do godz. 11:00**

   12.2. Otwarcie ofert nastąpi **w dniu 18.10.2024 r. o godz. 11:30** poprzez odszyfrowanie wczytanych na Platformie ofert”.

b) zmienia termin związania ofertą, tj. wykreśla dotychczasową treść pkt 9.1. SWZ i nadaje im nowe brzmienie:

   „9.1. Wykonawca będzie związany ofertą przez okres nie dłuższy niż **30 dni,** tj. **do dnia 15.11.2024r.”**

z-ca Dyrektora ds. Infrastruktury
Centrum Usług Informatycznych we Wrocławiu
Dariusz Dauksz

Dokument podpisano podpisem elektronicznym

Sporządziła: Lucyna Wdowik - Chlebek

Informacje na temat przetwarzania danych osobowych przez CUI znajdują się na stronie BIP CUI